

# 立法修改视角下的技术措施 保护范围

王 迁\*

**摘 要** 2020年《著作权法》直接纳入了《信息网络传播权保护条例》对技术措施的定义,导致防止未经许可运行计算机程序的“接触控制措施”和防止未经许可复制作品的“版权保护措施”被排除出保护范围,导致难以对计算机程序提供有效保护和与国际条约不符的后果。在再次修改《著作权法》之前,对此问题只能通过《著作权法实施条例》或司法解释对技术措施的扩大“解释”加以解决。2020年《刑法》规定规避技术措施入罪的用语在字面上未纳入对技术措施提供规避手段的行为,导致大大缩减了对技术措施的保护范围,使该条款基本失去意义。应根据《著作权法》和《信息网络传播权保护条例》中相同用语之间的关系,将《刑法》中的该用语解释为涵盖提供规避手段的行为。

**关键词** 技术措施 接触控制措施 版权保护措施 直接规避 提供规避手段

## 引 言

2020年11月和12月,我国《著作权法》和《刑法》先后完成了修订工作。修订的内容中均含有对技术措施的保护,说明立法者意识到了在数字时代技术措施对于维护著作权人利益的重要作用,并希望通过立法的修改提高对技术措施的民事保护水平并增加刑事保护。

其中,2020年修改后的《著作权法》(以下简称“2020年《著作权法》”)大幅增加了保护技术措施的条款。与2010年《著作权法》和2001年《著作权法》只含有一条有关规避技术措施法律

\* 华东政法大学教授。本文系国家自然科学基金重大项目“媒体融合中的版权理论与运用研究”(项目编号:19ZDA330)和教育部人文社会科学研究规划基金项目“网络游戏产业良性发展的版权保障研究”(项目编号:19YJA8200040)的阶段性成果。

责任的规定相比,〔1〕2020年《著作权法》对技术措施的含义与类别、〔2〕禁止对技术措施实施的行为〔3〕以及允许规避技术措施的例外情形均作出了规定,〔4〕内容大大丰富且构成了保护技术措施的完整体系。然而,对比2020年《著作权法》和2006年通过的《信息网络传播权保护条例》,不难发现前者中有关技术措施的条款基本照搬自《信息网络传播权保护条例》,除了部分文字调整之外,只增加了一项法定例外情形,即第50条第1款第(五)项规定的“进行加密研究或者计算机软件反向工程研究”。但是,《信息网络传播权保护条例》毕竟是旨在保护信息网络传播权的授权立法,其中涉及技术措施保护的条款也天然受此限制。将《信息网络传播权保护条例》中有关技术措施保护的条款简单地“升格”至《著作权法》,会大大限缩受保护的技术措施的类型,引起一系列立法者意料之外的连锁反应。

与此同时,经2020年《刑法修正案(十一)》修订后的《刑法》(以下简称“2020年《刑法》”),其第217条(“侵犯著作权罪”)首次将故意规避技术措施列为侵犯著作权罪的罪状之一。〔5〕然而,2020年《刑法》在列举该罪状时,没有采用2020年《著作权法》的相关表述,而是采用了2010年和2001年《著作权法》的表述,从而在字面上限缩了可入罪的规避技术措施的行为类型,使新增加的罪状基本失去意义。

由此可见,2020年《著作权法》和2020年《刑法》在保护技术措施方面的共同缺陷在于,其条款不合理地缩小了对技术措施的保护范围,前者表现在限缩了受保护的技术措施的类型,后者主要表现在限缩了可入罪的规避技术措施的行为类型。鉴于此,本文将分别梳理2020年《著作权法》和2020年《刑法》在此方面存在的问题,分析其成因和影响,并提出可能的解决方案,以合理地确定《著作权法》和《刑法》对技术措施的保护范围,从而实现两法之间的合理衔接。

## 一、2020年《著作权法》保护的技术措施类型

纵观各国著作权立法中技术措施的定义或保护技术措施的条款,可以发现受保护的技术措施大致可分类两种类型,即“接触控制措施”和“版权保护措施”。对这两类技术措施又可再进行更为细致的分类。

“接触控制措施”防止未经许可“接触”作品,按其功能可分为防止未经许可运行计算机程序的“接触控制措施”和防止未经许可阅读、欣赏其他作品或其他受保护的客体(以下简称“作品”)的“接触控制措施”。类似于门锁将房门锁闭,需要用钥匙开门,“接触控制措施”将作品“锁”了起来,只有获得了权利人许可(通常表现为向权利人付费)的使用者才能通过用户名、

〔1〕 参见2001年《著作权法》第47条第(六)项、2010年《著作权法》第48条第(六)项。

〔2〕 参见2020年《著作权法》第49条第3款。

〔3〕 参见2020年《著作权法》第49条第2款。

〔4〕 参见2020年《著作权法》第50条。

〔5〕 参见2020年《刑法》第217条第(六)项。

密码等类似于钥匙的验证信息,运行受保护的计算机程序或阅读、欣赏受保护的作品。例如,爱奇艺等视频网站要求用户用手机号注册并设定登录密码,在支付会员费后,才能点播或下载其中的影视剧。注册用户的手机号、密码和相应的验证机制就构成了“接触控制措施”。对于计算机程序权利人而言,“接触控制措施”更是其保护自身利益的主要技术手段。许多计算机程序可供用户免费下载并试用一段时间,但试用期过后,系统会提示输入相关账号进行身份验证。如果用户没有注册账号并支付费用,将无法正常运行,即无法调用(“接触”)计算机程序。再如,计算机程序开发商曾广泛使用俗称为“软件狗”或“加密狗”(dongle)的硬件设备,用户只有将其插入计算机的接口,且其验证计算机程序为正版或符合使用条件之后,用户才能正常运行,<sup>[6]</sup>因此其起到了类似“看家狗”的防止未经许可运行(“接触”)计算机程序的作用。

“版权保护措施”则用于阻止未经许可实施受专有权利控制的行为,按其保护的专有权利主要可分为防止未经许可复制作品的“版权保护措施”(以下简称为“防复制措施”)和防止未经许可通过网络传播作品的“版权保护措施”(以下简称为“防传播措施”)。20世纪八十年代应用在数字音乐中的“系列复制管理系统”(Serial Copy Management System)就是“版权保护措施”中典型的防复制措施。该系统在数字音乐被首次复制时,会在音乐复制件中插入特殊标记,与系统相兼容的数字录制设备可以检测数字音乐中是否有这段标记,如有则不予复制,以此确保原版音乐只能被复制一次,复制件不能被用于第二次复制。<sup>[7]</sup>电影DVD中的“内容扰乱系统”(Content Scrambling System,简称为CSS)可以防止将DVD中的电影复制到计算机硬盘上,或将该DVD进行翻刻,<sup>[8]</sup>也属于防复制措施。美国联邦通讯委员会曾经强制要求数字电视制造商使用的“广播标记”系统则是“版权保护措施”中典型的防传播措施。<sup>[9]</sup>该系统允许权利人在数字电视节目中加入一套被称为“广播标记”的特殊数据序列,与该系统相兼容的数字电视发现数字电视节目中含“广播标记”后,只会将数字电视节目输出到模拟录制设备或符合加密要求的数字设备中,从而起到了防止被录制的数字电视节目通过网络传播的作用。<sup>[10]</sup>

那么,2020年《著作权法》是否对这些类型的技术措施都提供了充分保护呢?通过对该法相关条款的分析,可以得出否定的结论。

### (一)不保护用于计算机程序的“接触控制措施”

对于2020年《著作权法》是否对“接触控制措施”提供了充分保护的问题,可举一例予以说

[6] 参见维基英文网站对“软件保护狗”(software protection dongle)的解释,see “Software protection dongle,” *Wikipedia*, [http://en.wikipedia.org/wiki/Software\\_protection\\_dongle#cite\\_note-0](http://en.wikipedia.org/wiki/Software_protection_dongle#cite_note-0), last visited on 10 February 2022.

[7] See House Report 102-873, Part 1, 102th Congress, 2nd Session, p. 9.

[8] CSS还具有其他功能,如确保只能在经过授权的设备上播放DVD,从而起到了“接触控制措施”的作用。

[9] 47 CFR § 73.9002, 9003, [Reserved by 76 FR 55818].

[10] See Federal Communications Commission, Digital Broadcast Content Protection, 68 FR 67624 (Nov 4, 2003).该行政法规现已被废止。

明。某人破解了大型商业制图软件中的正版验证机制,并编写了一个供用户破解该验证机制的程序供公众下载,试问该行为是否违反了2020年《著作权法》?相信多数人都不会不假思索地给出肯定的回答。然而,根据2020年《著作权法》对技术措施的定义,该假想例中的技术措施并不受保护。2020年《著作权法》第49条第3款规定:“本法所称的技术措施,是指用于防止、限制未经权利人许可浏览、欣赏作品、表演、录音录像制品或者通过信息网络向公众提供作品、表演、录音录像制品的有效技术、装置或者部件。”从中可以看出,其中的“接触控制措施”仅限于“用于防止、限制未经权利人许可浏览、欣赏作品、表演、录音录像制品”的技术措施,并不包括用于防止、限制未经权利人许可运行计算机程序的技术措施。

在上述假想例中,商业制图软件中的技术措施当然不能“用于防止、限制未经权利人许可浏览、欣赏”计算机程序,因为计算机程序就是代码化指令序列,<sup>[11]</sup>其作用在于指挥计算机等信息处理设备实现特定信息处理功能,并不用于“浏览、欣赏”。破解计算机程序中以“序列号”和相应的验证机制为代表的“接触控制措施”的目的,当然也不是去“浏览、欣赏”代码化指令序列,而是运行计算机程序,发挥其信息处理功能。

“接触控制措施”对于维护计算机程序权利人的利益而言最为重要。计算机程序与小说、音乐和绘画等文学艺术作品不同,其创作目的不是给人们带来精神上的愉悦或传递思想感情,而是完成特定信息处理工作。同时,计算机程序要发挥作用,必须以可被计算机读取的电子形式存在,而其他作品并非如此,如小说和绘画要展示思想感情或美感,通过纸张或其他物质载体即可,并不是必须采用电子形式。即使在数字时代,在计算机上创作的小说和绘画也可以通过印刷或以其他方式固定在纸张或其他物质载体上,从而被人们所阅读和欣赏。但计算机程序如果不以可被计算机读取的电子形式存在,就不可能指挥计算机完成信息处理工作。而以电子形式存在的计算机程序相较以其他形式存在的作品更容易被未经许可地利用,因此要维护计算机程序权利人的利益,就必须防止未经许可在计算机上复制和运行(“接触”)计算机程序。这就是为什么欧盟(原欧共体)直到2001年才在《版权指令》中保护用于所有类型作品的技术措施,<sup>[12]</sup>但早在1991年就在《计算机程序保护指令》中对用于计算机程序的技术措施提供保护。<sup>[13]</sup>在高速互联网时代来临之前,由于计算机程序主要是以磁盘或光盘等有体物为载体提供,不能将计算机程序拷贝到磁盘、光盘等存储介质上就不可能获得和运行计算机程序,因此对于维护计算机程序权利人的利益而言,当时计算机程序中的防复制措施与“接触控制措施”同样重要。但是,在当今的商业模式下,“接触控制措施”的重要性已经远超“版权保护

[11] 《计算机软件保护条例》第3条第(一)项规定:“计算机程序,是指为了得到某种结果而可以由计算机等具有信息处理能力的装置执行的代码化指令序列,或者可以被自动转换成代码化指令序列的符号化指令序列或者符号化语句序列……”

[12] See Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society, Article 6.

[13] See Council Directive 91/250/EEC of 14 May 1991 on the Legal Protection of Computer Programs, Article 7(1)(c).

措施”，这是因为计算机程序权利人已普遍将含有“接触控制措施”的计算机程序在其官网上免费向公众提供下载和试用。这就意味着对计算机程序的获取极为便捷，而且对含有“接触控制措施”的计算机程序的复制（下载和安装）是被权利人所允许的。计算机程序中防复制措施的重要性自然会下降。在计算机程序的试用期届满之后，“接触控制措施”就会发挥作用，未向计算机程序权利人支付费用的用户将无法继续正常运行计算机程序，或者无法调用全部功能。与此相适应，计算机程序权利人的主要收入就源于使用者为运行（“接触”）计算机程序所支付的费用。“接触控制措施”以此确保那些希望长期运行计算机程序或和调用其全部功能的用户向计算机程序权利人付费。可以想见，如果不对计算机程序中的“接触控制措施”提供法律保护，听任黑客破解此类技术措施并提供解密手段，计算机程序权利人的利益将受到极大的损害，对计算机程序的法律保护几近一句空话。

正因为如此，国外涉及计算机程序的技术措施保护的案例大多都针对规避“接触控制措施”的行为。如在美国发生的“微软公司诉银星微公司案”中，被告破解并出售运行 Windows 程序所必需的“序列号”，美国法院根据《千禧年数字版权法》关于禁止出售规避“接触控制措施”的手段的的规定，认定被告的行为违法。<sup>〔14〕</sup> 在“蓝港公司诉美国案”中，一名美国空军的雇员在其编写的人力数据管理程序中设置了“接触控制措施”，以确保许可期限届满后程序将无法运行，从而迫使用户下载新版本。美国空军未经许可聘用他人修改程序并去除了使用期限。从该雇员处受让计算机程序版权的蓝港公司起诉美国空军违反《千禧年数字版权法》中禁止规避“接触控制措施”的规定。<sup>〔15〕</sup> 再如，在澳大利亚发生的“索尼诉史蒂文斯案”中，原告索尼公司在 PlayStation 游戏机和游戏程序光盘中设有“控制码”系统，如果有人企图将盗版游戏光盘插入游戏机运行，会因为游戏机不能从光盘中读出与之相匹配的“控制码”而无法运行游戏。被告史蒂文斯则提供了用于破解“控制码”的“直读芯片”，使用户可以在游戏机中运行盗版游戏，由此引发诉讼。<sup>〔16〕</sup>

而在我国，迄今发生的与技术措施有关的案例中，绝大多数涉案行为都是规避计算机程序中的“接触控制措施”。如在“王锦峰等诉深圳市沙井沙一股份合作公司等案”中，原告采用“加密狗”和图像卡保护其开发的计算机操作系统。法院认定的事实是：“装载在上述机器中的软件，只有加密狗狗号与图像卡信息一致时，该装载软件才能运行，如果加密狗狗号与图像卡信息不一致，则该软件无法正常运行。”<sup>〔17〕</sup> 涉案技术措施显然就是防止未经许可运行计算机程

〔14〕 See Microsoft Corp. v. Silver Star Micro, Inc., 2008 U.S. Dist. LEXIS 1526. 当然，由于在运行 Windows 程序过程中会涉及对 Windows 程序在内存中的临时复制，因而在美国等承认临时复制为复制行为的国家中，该“序列号”也可以被视为“防复制措施”。但在此案中，原告只主张其“序列号”为“接触控制措施”。

〔15〕 See Blueport co v. United States, 533 F.3d 1374, 1376-1378 (Fed. Cir. 2008).

〔16〕 See Stevens v. Kabushiki Kaisha Sony Computer Entertainment and Others, [2005] HCA 58.

〔17〕 参见王锦峰等诉深圳市沙井沙一股份合作公司等侵犯计算机软件著作权案，广东省深圳市中级人民法院民事判决书，(2007)深中法民三初字第 160 号，广东省高级人民法院民事判决书，(2008)粤高法民三终字第 213 号。此案中原告诉称被告破解了软件中的技术措施，并复制软件后销售，但一审法院以原告证据不足为由驳回起诉。二审法院维持了一审法院的判决。

序的“接触控制措施”，被诉行为就是规避该技术措施。类似的案例还有“深圳市盈宁科技有限公司诉王海兵案”<sup>〔18〕</sup>“上海地创网络技术有限公司诉北京万户名媒科技有限公司上海分公司案”<sup>〔19〕</sup>和“北京文泰世纪科技公司诉孙晓峰等案”。<sup>〔20〕</sup> 假设对这些案件适用 2020 年《著作权法》，由于用于计算机程序的“接触控制措施”并不在该法保护的技术措施的范围内，无论是直接规避此种技术措施还是提供规避手段，认定这些行为违反《著作权法》将失去法律依据。

## （二）不保护“版权保护措施”中的防复制措施

对“接触控制措施”的保护存在重大缺失的 2020 年《著作权法》对“版权保护措施”也未能提供充分保护。对此也可举一例予以说明。假设某人破解了电影 DVD 中的防复制技术措施，并将解密方法公布在网络中，导致任何人都可以轻易将 DVD 中的电影复制到硬盘中。试问该行为是否违反了 2020 年《著作权法》？相信多数人不会不假思索地给出肯定的回答。

然而，2020 年《著作权法》对于“版权保护措施”中的防复制措施并不提供保护。《著作权法》第 49 条第 3 款定义的“版权保护措施”是指“用于防止、限制未经权利人许可……通过信息网络向公众提供作品、表演、录音录像制品的有效技术、装置或者部件。”从中可以看出，该“版权保护措施”仅限于用于保护信息网络传播权的“版权保护措施”，即防传播措施，并不涉及用于保护复制权的“版权保护措施”，也就是不保护防复制措施。在上文的假想例中，电影 DVD 中的技术措施是防复制措施，而不是防传播措施，因此并不属于 2020《著作权法》所保护的“版权保护措施”，破解该技术措施并提供解密手段并不违反 2020 年《著作权法》。

这样的结果当然是极不合理的。在多数情况下，对作品进行复制，是对作品进行其他利用的前提，因此用于防止复制的“版权保护措施”对保护权利人的利益具有极为重要的作用。时至今日，大多数“版权保护措施”都是防复制措施，至少都含有防止复制的功能。因此国外涉及“版权保护措施”的诉讼绝大多数都针对防复制措施。如在美国发生的“RealNetworks 诉 Streambox 案”中，RealNetworks 公司在其 RealServer 等计算机程序中采用了技术措施，权利人通过这些计算机程序在网络中提供作品时，可以设置为只允许用户在线欣赏而禁止下载。该技术措施是典型的防复制措施。Streambox 公司开发的程序能够规避该技术措施，用户可以借此下载作品。RealNetworks 公司起诉 Streambox 公司提供规避手段，法院认定 Streambox 公司违反了《千禧年数字版权法》有关禁止提供规避手段的规定并承担责任。<sup>〔21〕</sup> 在德国“CD 复制软件案”中，被告开发并销售专用于破解 CD 中防复制措施，以对 CD 进行复制的软件，德国联邦最高法院认定被告的行为违反了德国著作权法。<sup>〔22〕</sup> 而我国 2020 年《著作权法》

〔18〕 参见深圳市盈宁科技有限公司诉王海兵侵犯计算机软件著作权纠纷案，江苏省南通市中级人民法院民事判决书，(2005)通中民三初字第 0032 号。

〔19〕 参见上海地创网络技术公司等诉北京万户名媒科技公司侵犯计算机软件著作权纠纷案，上海市浦东新区人民法院民事判决书，(2008)浦民三(知)初字第 453 号。

〔20〕 参见北京文泰世纪科技公司诉孙晓峰等侵犯计算机软件著作权纠纷案，广东省深圳市龙岗区人民法院民事判决书，(2009)深龙法民初字第 4153 号。

〔21〕 See RealNetworks, Inc., v. Streambox, Inc., 2000 U.S. Dist. LEXIS 1889 (W.D. Wash. 2000).

〔22〕 Vgl. BGH NJW 2008, 3565 (3566).

将防复制措施排除在其定义的技术措施的范围之外,将使多数“版权保护措施”无法受到《著作权法》的保护。

上文已经指出,2020年《著作权法》在技术措施的定义中排除了用于计算机程序的“接触控制措施”,再加之该定义又排除了所有的防复制措施,用于计算机程序的唯一受保护的技术措施就剩下了“版权保护措施”中的防传播措施。但由于目前计算机程序权利人采用的商业模式多为在官网上免费提供计算机程序的下载和试用,同时在试用期届满后要求用户付费购买使用许可。这就意味着在网上传播含有此类含有“接触控制措施”的计算机程序本身(其中的“接触控制措施”未被破解)并不会严重损害计算机程序权利人的利益,《著作权法》对用于计算机程序的技术措施的保护也就基本丧失了存在价值。

## 二、升格《信息网络传播权保护条例》中技术措施的定义属于“改劣”

对于2020年《著作权法》保护技术措施范围存在的明显缺陷,可能存在的一种解释是,该缺陷并不源于2020年对《著作权法》的修改,而是源于《信息网络传播权保护条例》,因为2020年《著作权法》对技术措施的定义完全来源于《信息网络传播权保护条例》,只是将该条例中有关技术措施定义的原有缺陷带入了《著作权法》。但该解释是不能成立的,可以说,2020年修改《著作权法》时将《信息网络传播权保护条例》中技术措施的定义原封不动地纳入(也就是将其“升格”)属于“改劣”,较之2010年《著作权法》反而会造成立法者始料不及的后果。

### (一)《信息网络传播权保护条例》对技术措施“不完整”定义的合理性

《信息网络传播权保护条例》第26条第2款规定:“本条例下列用语的含义:……技术措施,是指用于防止、限制未经权利人许可浏览、欣赏作品、表演、录音录像制品的或者通过信息网络向公众提供作品、表演、录音录像制品的有效技术、装置或者部件。”该定义也没有包含用于计算机程序的“接触控制措施”以及“版权保护措施”中的防复制措施,但是,这并不属于《信息网络传播权保护条例》在立法上的失误。

2006年制订的《信息网络传播权保护条例》的性质是授权立法,其来源于2001年《著作权法》第58条——“计算机软件、信息网络传播权的保护办法由国务院另行规定。”作为授权立法,《信息网络传播权保护条例》仅仅是“信息网络传播权的保护办法”,并不能用于保护复制权或其他专有权利,当然也不能对用于保护复制权或其他专有权利的“版权保护措施”提供保护。在《信息网络传播权保护条例》的起草过程中,曾有意见认为应当对“临时复制”作出规定。<sup>[23]</sup>但负责条例起草的国务院法制办公室认为:“作为授权立法,条例也不宜对著作权法未授权的

[23] 《信息网络传播权保护条例》(2005年7月版草案)第3条(复制权)规定:“著作权法……规定的复制权,适用于以任何方法或者形式对作品、表演或者录音录像制品进行的永久或者暂时的、全部或者部分的复制。”该规定实际上承认了“临时复制”为“复制行为”。

临时复制作出规定。因此,条例对临时复制未作规定。”<sup>[24]</sup>

虽然未经许可对文学艺术作品的浏览和欣赏(“接触”文学艺术作品)并不直接属于信息网络传播权规制的行为,但《信息网络传播权保护条例》第26条第2款界定技术措施时使用的“浏览”实际上特指网络浏览。使他人通过网络浏览和欣赏文学艺术作品,是通过信息网络对此类作品进行交互式传播的主要目的。对于未经许可通过网络提供的受“接触控制措施”保护的作品,只要其中的技术措施未被破解,他人未经权利人许可就无法浏览、欣赏,该作品不会吸引多少用户,也不会有多少人去提供。因此,只要能够有效保护文学艺术作品中的“接触控制措施”,就能在很大程度上防止未经许可提供文学艺术作品的浏览和欣赏,也就间接保护了文学艺术作品的信息传播权。与此同时,著作权法中也没有所谓的“接触权”,<sup>[25]</sup>对文学艺术作品的浏览和欣赏也不可能属于任何其他专有权利规制的行为,《信息网络传播权保护条例》保护“用于防止、限制未经权利人许可浏览、欣赏作品”的技术措施也与其他专有权利无关。因此在《信息网络传播权保护条例》中规定与信息网络传播权的保护有关的、用于防止文学艺术作品被未经许可浏览和欣赏的“接触控制措施”是有合理性的。

与此形成鲜明对比的是,在2006年《信息网络传播权保护条例》制定之时,计算机程序主要是通过磁盘、光盘等存储介质向用户提供的,计算机程序权利人通过网络提供试用版程序的商业模式远未成为常态。因此在当时保护计算机程序中的“接触控制措施”与保护计算机程序的信息网络传播权之间的关系并不密切,《信息网络传播权保护条例》未将计算机程序中的“接触控制措施”纳入保护范围,同样具有合理性。

由此可见,《信息网络传播权保护条例》之所以在定义技术措施时未纳入防止计算机程序被未经许可运行的“接触控制措施”,也未纳入“版权保护措施”中的防复制措施,是由其授权立法的性质所决定的。该条例的制定者是刻意而非出于疏忽为技术措施下了一个并不完整的定义,其根本原因正是该条例所保护的技术措施必须与信息网络传播权的保护存在关联。

特别需要指出的是,《信息网络传播权保护条例》中技术措施定义的“不完整”,不但没有导致用于计算机程序的“接触控制措施”以及“版权保护措施”中的防复制措施被排除出2001年和2010年《著作权法》的保护范围,而且还可以印证这两类技术措施是在当时的《著作权法》保护范围之内的。这是由于2001年和2010年《著作权法》中均没有包含技术措施的定义,只对规避技术措施的法律责任作了规定,<sup>[26]</sup>因此对受其保护的技术措施的范围必须进行解释。《信息网络传播权保护条例》作为授权立法和行政法规,对技术措施的保护范围不可能超越《著

[24] 参见“国务院法制办公室负责人就《信息网络传播权保护条例》答《中国政府法制信息网》记者问”,载张建华主编:《信息网络传播权保护条例释义》,中国法制出版社2006年版,第108页。

[25] 在《著作权法》明确赋予著作权人的十六项专有权利中,没有一项能够控制以阅读方式“接触”作品内容行为。因此购买和阅读盗版书籍并不构成对著作权的侵害。英国最高法院在2013年的一项判决中指出:“一个人阅读受保护作品的盗版,或者是观赏伪造的受保护的油画,并不构成侵权,虽然向此人销售该盗版或伪造油画的人可能实施了侵权行为。”Public Relations Consultants Association Limited v. the Newspaper Licensing Agency Limited and others, [2013] UKSC 18, para. 1.

[26] 参见2001年《著作权法》第48条第(六)项、2010年《著作权法》第48条第(六)项。

作权法》的规定,否则既超出了《著作权法》授权的范围,也会导致作为下位法的行政法规违反作为上位法的法律的严重后果。负责起草《信息网络传播权保护条例》的国务院法制办公室对此明确指出:该条例“应当以《著作权法》的有关规定为基础,……条例的规定应当与《著作权法》有关规定保持一致,……不得超越《著作权法》规定的基本制度”。〔27〕

既然《信息网络传播权保护条例》定义的技术措施既包含“接触控制措施”又包含“版权保护措施”,就说明 2001 年和 2010 年《著作权法》所保护的技术措施必然包括这两类技术措施。换言之,《信息网络传播权保护条例》保护的技术措施可以比 2001 年和 2010 年《著作权法》保护的技术措施在范围上更小,但绝不可能更大。那些与信息网络传播权的保护关系不大、不能受到《信息网络传播权保护条例》保护的“接触控制措施”和“版权保护措施”,当然属于 2001 年和 2010 年《著作权法》所保护的技术措施的范围。这样一来,用于防止未经许可运行计算机程序的“接触控制措施”和用于“版权保护措施”中的防复制措施都应由 2001 年和 2010 年《著作权法》进行保护。

对于上述结论,还可以从《计算机软件保护条例》的规定和相关司法实践得到印证。《计算机软件保护条例》第 24 条第 1 款第(三)项将“故意避开或者破坏著作权人为保护其软件著作权而采取的技术措施”列为侵权行为。虽然《计算机软件保护条例》也没有对受其保护的技术措施的范围进行界定,但可以确定的是,该《条例》保护的用于计算机程序的技术措施不可能仅限于保护信息网络传播权的“版权保护措施”,否则就会与《信息网络传播权保护条例》对防止未经许可通过网络传播作品的技术措施的保护完全重叠。导致《计算机软件保护条例》对技术措施的保护丧失其存在的意义。鉴于上文所述的“接触控制措施”对维护计算机程序权利人利益的重大意义,再加之 2001 年《计算机软件保护条例》增加保护技术措施的条款时,“版权保护措施”中的防复制措施仍然在发挥防止未经许可拷贝计算机程序的重要作用,《计算机软件保护条例》所保护的技术措施当然包括防止未经许可运行程序的“接触控制措施”和防止未经许可拷贝程序的防复制措施。《计算机软件保护条例》同样是授权立法,其对计算机程序中技术措施的保护范围,也不可能超过 2001 年和 2010 年《著作权法》保护的技术措施的范围。这同样可以说明 2001 年和 2010 年《著作权法》所保护的技术措施必然包括所有的“接触控制措施”和“版权保护措施”。

司法实践也印证了上述结论。对于计算机程序中防止未经许可运行程序的“接触控制措施”,法院也正是根据 2001 年或 2010 年《著作权法》和《计算机软件保护条例》来提供保护的。如在“上海地创网络技术有限公司诉北京万户名媒科技有限公司上海分公司案”中,计算机程序权利人在计算机程序中使用了“接触控制措施”,用于防止许可期届满后,用户在未付费的情况下继续运行该程序。该案被告在其获得的许可到期后,为了能继续运行程序,采用技术手段破解了该技术措施。法院认定被告承担法律责任的法律依据之一,是 2001 年《著作权法》第 47 条第(六)项(即 2010 年《著作权法》第 48 条第(六)项)和《计算机软件保护条例》第 24 条第

〔27〕 张建华,见前注〔24〕,第 4 页。

1款第(三)项,<sup>[28]</sup>而这两条规定的正是规避技术措施所导致的法律责任。由此可见,法院认为2001年和2010年《著作权法》及《计算机软件保护条例》所保护的技术措施当然包括计算机程序中的“接触控制措施”。

## (二)升格《信息网络传播权保护条例》中技术措施定义的后果

2020年在修改《著作权法》时,将《信息网络传播权保护条例》中对技术措施的不完整定义简单地升格至《著作权法》,而没有考虑到《信息网络传播权保护条例》作为授权立法的性质及其与《著作权法》的关系,从而导致了超出立法者预期的后果。

当上述对技术措施的不完整定义仅仅出现在《信息网络传播权保护条例》中,且《著作权法》本身没有对技术措施下定义之时。基于《信息网络传播权保护条例》授权立法的性质,尚且可推定其保护的技术措施完全包含在《著作权法》保护的技术措施范围之内,也就是2001年和2010年《著作权法》保护的技术措施在范围上远大于《信息网络传播权保护条例》。然而,2020年《著作权法》直接纳入了对技术措施的上述不完整定义,这就意味着2020年《著作权法》保护的技术措施在范围上仅限于此,也就是2020年《著作权法》对技术措施的保护范围与《信息网络传播权保护条例》完全相同,不存在前者大于后者的可能。

2020年《著作权法》对技术措施的不完整定义,同时堵死了对《计算机软件保护条例》所保护的技术措施的范围进行合理解释的路径。如上文所述,《计算机软件保护条例》没有对技术措施进行定义,但由于2001年和2010年《著作权法》没有对技术措施的范围进行限定,再加之《信息网络传播权保护条例》对“接触控制措施”和“版权保护措施”都提供了保护(虽然是不完整的保护),可以推定2001年和2010年《著作权法》对这两类技术措施必然都提供保护,进而推定《计算机软件保护条例》保护的用于计算机程序的技术措施既包括防止未经许可运行程序的“接触控制措施”,也包括“版权保护措施”中的防复制措施。然而,作为授权立法和行政法规的《计算机软件保护条例》对技术措施的保护范围不可能超越《著作权法》的规定。既然2020年《著作权法》已明确将其保护的“接触控制措施”限定为“用于防止、限制未经权利人许可浏览、欣赏”的技术措施,将其保护的“版权保护措施”限定为“用于防止、限制未经权利人许可通过信息网络向公众提供”的技术措施,就不能再将《计算机软件保护条例》所保护的用于计算机程序的技术措施解释为包括防止未经许可运行计算机程序的“接触控制措施”和防止未经许可拷贝计算机程序的防复制措施,否则将导致对2020年《著作权法》的违反。这样一来,保护那些防止未经许可运行计算机程序的“接触控制措施”和防止未经许可复制计算机程序的“版权保护措施”在我国就完全丧失了法律依据。

2020年《著作权法》对技术措施的不完整定义还引起了著作权保护体系的混乱。如本文开篇所述,2020年《著作权法》对技术措施的规定基本都是从《信息网络传播权保护条例》的规定“升格”而来,新增加的只有一项允许规避技术措施的例外情形——“进行加密研究

[28] 参见上海地创网络技术公司等诉北京万户名媒科技公司侵犯计算机软件著作权纠纷案,上海市浦东新区人民法院民事判决书,(2008)浦民三(知)初字第453号。

或者计算机软件反向工程研究”。〔29〕既然是为了进行“计算机软件反向工程研究”而规避技术措施,该技术措施只可能是用于防止计算机程序被未经许可运行的“接触控制措施”或防止程序被复制的“版权保护措施”。参与立法者对此项例外清楚地指出:“诸多软件开发都会在其开发的软件之上施加技术保护措施以防止他人未经许可接触(即运行)有关软件,若不对此规定例外,则很容易削弱其他软件爱好者或有关组织对不同软件兼容性进行研究的兴趣。”〔30〕然而,此类技术措施根本就不在2020年《著作权法》保护的范围之内,规定此项例外情形岂不是多此一举?

与此同时,由于计算机程序不是用于被浏览和欣赏的,并不存在“用于防止、限制未经权利人许可浏览、欣赏”计算机程序的“接触控制措施”,在2020年《著作权法》限定的范围内,《计算机软件保护条例》所保护的技术措施就只剩下了“用于防止、限制未经权利人许可通过信息网络向公众提供”计算机程序的“版权保护措施”(即防传播措施)。然而,无论是《著作权法》还是《信息网络传播权保护条例》对于此类技术措施的保护并不区分作品类型,其中当然包括用于防止计算机程序被未经许可通过信息网络提供的“版权保护措施”。这就意味着《计算机软件保护条例》对技术措施的保护完全被《著作权法》和《信息网络传播权保护条例》所覆盖,已经没有存在的必要性了。

2020年《著作权法》中技术措施定义的上述缺陷也不可避免地影响了2020年《刑法》对技术措施的保护范围。根据2020年《刑法》第217条第(六)项的规定,“未经著作权人或者与著作权有关的权利人许可,故意避开或者破坏权利人为其作品、录音录像制品等采取的保护著作权或者与著作权有关的权利的技术措施”可构成“侵犯著作权罪”。《刑法》第217条规定的是“侵犯著作权罪”,其中所保护的技术措施,当然应与《著作权法》所保护的技术措施具有相同的含义和范围,将规避技术措施行为认定为“侵犯著作权罪”并追究行为人刑事责任的前提,理应是该行为根据《著作权法》构成违法,〔31〕行为人应承担民事责任。〔32〕既然2020年《著作权法》将用于计算机程序的“接触控制措施”和“版权保护措施”中的防复制措施排除出了保护范围,也就是规避这两类技术措施的行为并不违反2020年《著作权法》、并不导致民事责任,那么

〔29〕 2020年《著作权法》第50条第1款第(五)项。

〔30〕 黄薇、王雷鸣主编:《中华人民共和国著作权法导读与释义》,中国民主法制出版社2021年版,第252页。

〔31〕 修改前后的《著作权法》均将规避技术措施行为列为“侵权行为”,参见2010年《著作权法》第48条第(六)项、2020年《著作权法》第53条第(六)项。但严格意义上的著作权侵权行为是指未经许可实施复制、交互式网络传播等受复制权、信息网络传播权等专有权利规制的行为,而规避技术措施本身并不受任何专有权利规制,并不属于对著作权专有权利的“侵权”,而是属于违反著作权法规定的违法行为。国外著作权立法也均将规避技术措施定为“违法”而非“侵权”。

〔32〕 在保护著作权的刑事司法实践中,有一种观点认为,即使一种行为不可能根据《著作权法》构成侵权行为并被追究民事责任,也可以根据《刑法》217条入罪;《刑法》217条中涉及“侵犯著作权罪”中的用语,可以与《著作权法》中的相同术语具有不同的意思。参见李小文、杨永勤:“网络环境下复制发行的刑法新解读”,《中国检察官》2013年第3期,第21页。笔者不赞同该观点。参见王迁:“论著作权保护刑民衔接的正当性”,《法学》2021年第8期,第14—17页。

该行为也不可能构成“侵犯著作权罪”并导致刑事责任。这样一来,2020年《刑法》将规避技术措施的行为入罪的意义势必将大打折扣。

更为严重的是,修改后的《著作权法》对技术措施所界定的保护范围与相关国际条约的规定不符。2001年《著作权法》修改时之所以增加对技术措施的保护,直接动因是1996年世界知识产权组织主持缔结的《世界知识产权组织版权条约》(简称WCT)和《世界知识产权组织表演和音制品条约》(简称WPPT)规定了保护技术措施的义务。虽然2001年我国尚未加入两条约,但着眼未来,也以两条约作为参考,规定了对技术措施的保护。2007年两条约对我国生效后,我国则负有按照条约的要求保护技术措施的义务。《世界知识产权组织版权条约》第11条(关于技术措施的义务)规定:“缔约各方应规定适当的法律保护和有效的法律补救办法,制止规避由作者为行使本条约或《伯尔尼公约》所规定的权利而使用的、对就其作品进行未经该有关作者许可或未由法律准许的行为加以约束的有效技术措施。”《世界知识产权组织表演和音制品条约》第18条也以基本相同的用语规定了对用于表演和录音制品的技术措施的保护。

《世界知识产权组织版权条约》规定的“由作者为行使本条约或《伯尔尼公约》所规定的权利而使用的……技术措施”当然包括为行使该条约规定的所有专有权利而使用的“版权保护措施”。特别是由于《伯尔尼公约》和《世界知识产权组织版权条约》都规定了复制权,<sup>[33]</sup>而且“版权保护措施”中的防复制措施是最为常见和重要的“版权保护措施”,两条约当然要求保护此类技术措施。

对此,世界知识产权组织编写的《世界知识产权组织管理的版权和相关权条约指南及版权及相关权术语汇编》在解释《世界知识产权组织版权条约》第11条(关于技术措施的义务)时,将“防止未经许可复制”的技术措施作为条约所保护的技术措施的典型实例。<sup>[34]</sup>但是,按照2020年《著作权法》对技术措施的定义,“版权保护措施”中的防复制措施被完全排除出了受保护范围,从而导致我国对技术措施的保护水平与两条约不符。这恐怕又是立法者“升格”技术措施的定义时所未曾预料到的后果。

由此可见,将《信息网络传播权保护条例》中对技术措施的不完整定义“升格”至2020年《著作权法》中,其效果较之前更差,属于“改劣”。对此最佳的解决方案当然是及时修改《著作权法》,完善对技术措施的定义,将用于防止未经许可运行计算机程序的“接触控制措施”和“版权保护措施”中的防复制措施都纳入其中。然而自《著作权法》于1990年颁布至今,只经历过

[33] 《伯尔尼公约》第9条第1款规定:“受本公约保护的文学艺术作品的作者,享有授权以任何方式和采取任何形式复制这些作品的专有权利。”《世界知识产权组织版权条约》第1条第(4)款规定:“缔约各方应遵守《伯尔尼公约》第1至21条和附件的规定。”关于该条的“议定声明”还规定:“《伯尔尼公约》第9条所规定的复制权及其所允许的例外,完全适用于数字环境,尤其是以数字形式使用作品的情况。不言而喻,在电子媒体中以数字形式存储受保护的作品,构成《伯尔尼公约》第9条意义下的复制。”

[34] See WIPO, *Guide to Copyright and Related Rights Treaties Administered by WIPO and Glossary of Copyright and Related Rights Terms*, WIPO publication No. 891(E), 2003, p. 216.

三次修改,每次间隔期间平均为10年,<sup>[35]</sup>而且2010年的修改只是对《著作权法》的微调。如果保持这样的修改频率,则距下一次修改还有10年左右的时间,这当然是“远水解不了近渴”。更为严重的是,2020年《著作权法》对技术措施的定义是封闭型的,没有使用“等”或其他开放式用语,且范围非常清楚、明确。无论用何种法律解释方法,都不可能从中解释出其包含用于防止未经许可运行计算机程序的“接触控制措施”和“版权保护措施”中的防复制措施。

在《著作权法》下次修改之前,作为权宜之计,笔者建议先修改《著作权法实施条例》或由最高人民法院发布司法解释,对受2020年《著作权法》保护的技术措施的类型进行超出其字面含义的“解释”,以纳入防止未经许可运行计算机程序的“接触控制措施”和防止未经许可复制的“版权保护措施”。当然,严格地说,这已经不是“解释”2020年《著作权法》,而是实质性地修改2020年《著作权法》,与制定行政法规和司法解释的权限不符。然而,所谓“两害相权取其轻”,在迫不得已的情况下,特别是为了避免我国违反国际条约规定的义务,在《著作权法》下一次修订之前,这可能是唯一现实的解决方案。

### 三、2020年《刑法》规定的规避技术措施入罪的行为类型

即使上文建议的解决方案得到采纳,使2020年《著作权法》保护的技术措施涵盖用于计算机程序的“接触控制措施”以及“版权保护措施”中的防复制措施,从而使对上述类型技术措施的规避也可构成违反2020年《著作权法》的行为,并在达到入罪门槛时根据2020年《刑法》被定为刑事犯罪,2020年《刑法》中规避技术措施可入罪的行为范围仍然可能因其条款的用语问题而被不合理地限缩。

《世界知识产权组织版权条约》第11条和《世界知识产权组织表演和录音制品条约》第18条要求“制止规避……技术措施”。对于何为“规避”,两条约本身并没有做出明确规定。从各国立法的情况来看,“规避”包含两种形式,一是动手破解相关的技术措施,也被称为“直接规避”;二是制造和向他人提供规避设备、工具或服务(以下简称“提供规避手段”),也被称为“间接规避行为”。<sup>[36]</sup>那么,2020年《著作权法》和2020年《刑法》是否对这两类行为都予以禁止呢?

#### (一)对可入罪的规避技术措施的行为范围的疑问

对于上述问题,2020年《著作权法》给出了肯定的回答,其第49条第2款规定:“未经权利人许可,任何组织或者个人不得故意避开或者破坏技术措施,不得以避开或者破坏技术措施为目的制造、进口或者向公众提供有关装置或者部件,不得故意为他人避开或者破坏技术措施提供技术服务。……”其中,“故意避开或者破坏技术措施”显然就是“直接规避”,“以避开或者破

[35] 《著作权法》分别于2001年、2010年和2020年修订。

[36] 在国务院法制办公室编写的《信息网络传播权保护条例释义》中,有如下表述:“规避技术措施的行为包括三类:一是避开或者破坏技术措施……二是制造、进口或者向公众提供主要用于避开或者破坏技术措施的装置或者部件……三是为他人避开或者破坏技术措施提供技术服务……上述三类行为中,第一类属于直接规避技术措施的行为……第二、三类属于间接规避技术措施的行为。”张建华,见前注[24],第16—17页。

坏技术措施为目的制造、进口或者向公众提供有关装置或者部件”以及“故意为他人避开或者破坏技术措施提供技术服务”则属于“提供规避手段”。可见,2020年《著作权法》同时禁止这两类行为。

与之形成对比的是,从2020年《刑法》的字面意思看,对上述问题的回答则是否定的。其第217条第(六)项规定:“未经著作权人或者与著作权有关的权利人许可,故意避开或者破坏权利人为其作品、录音录像制品等采取的保护著作权或者与著作权有关的权利的技术措施”可构成“侵犯著作权罪”。其中只提及“故意避开或者破坏技术措施”,并未纳入“以避开或者破坏技术措施为目的制造、进口或者向公众提供有关装置或者部件”以及“故意为他人避开或者破坏技术措施提供技术服务”。这不可避免地使人产生一个印象:根据2020年《刑法》,只有“直接规避”才能入罪,“提供规避手段”不能入罪。

对比修改前后《著作权法》有关规避技术措施责任的规定,上述印象会进一步得到加强。2010年《著作权法》第48条规定:“有下列侵权行为的,……(六)未经著作权人或者与著作权有关的权利人许可,故意避开或者破坏权利人为其作品、录音录像制品等采取的保护著作权或者与著作权有关的权利的技术措施的……”(2001年《著作权法》第47条第(六)项有相同规定);2020年《著作权法》第53条规定:“有下列侵权行为的,……(六)未经著作权人或者与著作权有关的权利人许可,故意避开或者破坏技术措施的,故意制造、进口或者向他人提供主要用于避开、破坏技术措施的装置或者部件的,或者故意为他人避开或者破坏技术措施提供技术服务的……”(着重号为笔者所加)。显然,“提供规避手段”的法律责任,是在2020年修改《著作权法》时才明确规定的。这自然容易使人认为2010年《著作权法》第48条和2001年第47条规定的规避技术措施的法律责任,仅限于“直接规避”的法律责任,因此2020年《刑法》与之类似,只有“直接规避”才可构成犯罪。那么,这一解释能否成立呢?

## (二)可入罪的规避技术措施行为不限于“直接规避”

笔者认为,上述解释会使2020年《刑法》规定规避技术措施入罪的规定意义寥寥,不可能反映真实的立法意图,因此是不可取的。

首先,在不向公众提供规避手段的情况下,仅仅实施“直接规避”对权利人的利益造成的损害并不大。“直接规避”的直接后果,当然是使作品失去其技术保护层,从而可被未经许可地“接触”或复制、通过网络传播等。如果后续利用是面向公众发行或传播作品,比如在破解了计算机程序中的序列号之后,将去除序列号后的计算机程序通过网络销售(付费下载),或破解电影DVD中的防复制措施后,将电影拷贝到硬盘上并销售装有电影的硬盘,或者提供电影的网络点播或下载,则这些后续利用构成对复制权、发行权或信息网络传播权的侵害。此时即使《刑法》并未将“直接规避”列为罪状,上述后续利用行为只要达到了入罪门槛,仍可被定为“侵犯著作权罪”。<sup>[37]</sup>那么《刑法》规定“直接规避”构成刑事犯罪的意义又在哪里呢?

[37] 修改后的《刑法》第217条第(一)项将“未经著作权人许可,复制发行、通过信息网络向公众传播其文字作品、音乐、美术、视听作品、计算机软件及法律、行政法规规定的其他作品”列为“侵犯著作权罪”的罪状。

如果对计算机程序中防止未经许可运行的“接触控制措施”实施“直接规避”后,自行对计算机程序进行未经许可的商业使用,也就是商业性运行盗版,则该商业使用行为依最高人民法院的司法解释构成对复制权的民事侵权。<sup>[38]</sup> 根据相关刑事司法解释,《刑法》第 217 条可适用于单独侵犯复制权的行为,<sup>[39]</sup>但 2020 年《刑法》增加规避技术措施入罪的规定,不可能只是为了对“直接规避”计算机程序中“接触控制措施”后自己运行该程序的行为进行刑事打击。其原因在于,如果商业性运行盗版程序因被认定为侵犯复制权而入罪,则同时将作为该行为预备行为的“直接规避”定为犯罪并无多少实际意义;如果不认为商业性运行盗版程序可以入罪,则仅作为该行为预备行为的“直接规避”就更不应当被认定为犯罪了。事实上,在此前的刑事司法实践中,也从未出现将商业性运行盗版程序认定为侵犯复制权并追究刑事责任的案例。

在上文提及的“上海地创网络技术公司等诉北京万户名媒科技公司案”中,作为企业的被告破解了计算机程序的序列号,以便在许可期限届满后继续运行该程序。该案被告对计算机程序先后实施了两个行为——先规避“接触控制措施”(即“直接规避”),再未经许可商业使用计算机程序。从法律定性上,这当然是两个独立的行为,前者构成违法,后者侵犯专有权利(复制权)。<sup>[40]</sup> 但是,由于前一行行为本质上是后者的预备行为,而对后一行行为被告本来就应当承担停止侵权和赔偿损失的侵权责任。前一行行为并没有给权利人带来额外的损失,法院认定前一行行为构成违法在此类案件中也仅有宣示意义。即使本案被告没有自己动手规避技术措施,而是从他人手中购得已清除技术措施的盗版计算机程序并运行,被告未经许可商业使用计算机程序构成侵权的性质并不会改变,被告向权利人支付的赔偿金数额也不会发生变化。如果将此案改为刑事案件,假设后一行行为(运行盗版程序侵犯复制权)已被定为侵犯著作权罪,又有何必要再将前一行行为(为自用盗版而规避技术措施)也认定为侵犯著作权罪呢? 假设后一行行为都未被定罪,仅仅是为后一行行为做准备的前一行行为又怎么会被定罪呢?

如果实施“直接规避”后对作品的后续利用属于纯粹的私人使用,如破解计算机程序中的序列号后非商业性运行程序,或者破解电影 DVD 中的防复制措施后,将电影拷贝到硬盘上供自己或家人欣赏,则这些后续使用行为属于合理使用,并不构成侵权。<sup>[41]</sup> 这些行为当然也会损害权利人的利益,只是其造成的损害就是一份作品许可费的损失,与规避者为个人使用而直接购买并运行盗版计算机程序,或阅读盗版文学艺术作品无异,与向公众提供规避手段,导致不特定多数人都可以自行规避技术措施并对作品进行未经许可的利用导致的损害后果是无法相提并论的。在后续的私人使用既不可能构成刑事犯罪,也不可能构成民事侵权的情况下,由

[38] 参见《最高人民法院关于审理著作权民事纠纷案件适用法律若干问题的解释(2020 修正)》第 21 条。

[39] 《最高人民法院 最高人民检察院关于办理侵犯知识产权刑事案件具体应用法律若干问题的解释(二)》第 2 条规定:“刑法第二百一十七条侵犯著作权罪中的‘复制发行’,包括复制、发行或者既复制又发行的行为。”据此,单独实施的复制行为也可能入罪。

[40] 参见上海地创网络技术公司等诉北京万户名媒科技公司计算机侵犯软件著作权纠纷案,上海市浦东新区人民法院民事判决书,(2008)浦民三(知)初字第 453 号。

[41] 参见《著作权法》第 24 条第 1 款第(一)项。

同一行为人为自己私人使用而实施的“直接规避”当然不应被认定为刑事犯罪。因此,2020年《刑法》将规避技术措施定为犯罪时,不可能针对此类行为。

正因为如此,有些国家根本就不认为世界知识产权组织的两个条约要求禁止“直接规避”,它们也只在著作权立法中禁止提供规避手段,而不禁止“直接规避”,其典型代表为澳大利亚2000年《数字议程法案》、<sup>[42]</sup>日本1999年《著作权法》<sup>[43]</sup>以及2008年新西兰《版权法》。<sup>[44]</sup>在这些立法中,“直接规避”甚至都不会导致民事责任,更遑论刑事责任了。

与“直接规避”相比,向公众提供规避手段对权利人利益的损害显然要大得多,因为这将使不具备专业技术能力的普通人也能自己动手规避技术措施且未经许可运行计算机程序或阅读、欣赏文学艺术作品。两者之间的差距,类似于自己在家中阅读盗版小说和通过网络提供该小说的下载。因此,凡是世界知识产权组织两条约的缔约方都在立法中禁止对技术措施提供规避手段,即使是那些不禁止“直接规避”的立法也是如此,如澳大利亚2000年《数字议程法案》、日本1999年《著作权法》和2008年新西兰《版权法》均禁止对受保护的技术措施提供规避手段。

前文提及,欧盟早在1991年颁布的《计算机程序保护指令》中就对用于计算机程序的技术措施提供保护,但保护方法是禁止提供规避手段,并不包括禁止“直接规避”。<sup>[45]</sup>世界知识产权组织两条约有关保护技术措施的条款在草案中也只针对提供规避手段,并不针对“直接规避”,<sup>[46]</sup>说明禁止提供规避手段而非禁止“直接规避”才是条约起草者希望实现的目的。虽然在1996年为缔结两条约而召开的外交会议上,两条约中保护技术措施的条款使用了更为概括的用语,即“制止规避”,没有明确提及禁止提供规避手段,但世界知识产权组织编写的《世界知识产权组织管理的版权与相关权条约指南》强调,只有对那些使规避行为能够实现的“预备行为”(即制造、进口和散发规避工具和为规避而提供服务)规定法律责任,缔约方才能履行《世界

[42] See Digital Agenda Act, Section 116A. “澳大利亚数字联盟”对此表示:仅禁止提供用于规避技术措施的设备和服 务,而不禁止(直接)规避技术措施的行为,完全符合澳大利亚所承担的国际义务。See Australian Digital Alliance, Copyright Amendment (Digital Agenda) Bill 1999: Response from the Australian Digital Alliance (ADA), pp. 1-2.

[43] See Japan Copyright Law (1999), Article 120bis(i)(ii).

[44] See New Zealand Copyright Act, 226A.

[45] 该《指令》规定:“对于任何唯一设计目的在于为未经许可移除或规避用于保护计算机程序的技术设备提供便利的工具,如为商业目的持有,或将其投入流通领域,则成员国应当提供适当的救济措施。”See Directive on the Legal Protection of Computer Programs, Article 7(1)(c).

[46] 《世界知识产权组织版权条约》草案第13条规定:“①缔约方应当将进口、制造或散发用于规避(技术措施)的设备的行为,或提供、实施能达到相同效果的服务行为定为非法,只要任何人知道或有合理理由知道该设备或服务将被用于行使本条约规定的,而未经权利人或法律授权的权利。②缔约方应当针对第(1)款规定的非法行为提供适当和充分的救济措施。”《世界知识产权组织表演和录音制品条约》草案第22条用相同措辞规定了对表演者和录制者使用的技术措施的保护。

知识产权组织版权条约》第 11 条规定的义务。<sup>[47]</sup> 对此,国际学术界较为权威的著作也持相同观点。<sup>[48]</sup>

由此可见,虽然《信息网络传播权保护条例》和 2020 年《著作权法》同时禁止“直接规避”和提供规避手段,并对这两种行为都规定了法律责任,但打击的重点当然是提供规避手段,而非“直接规避”。如果认为根据 2020 年《刑法》,只有“直接规避”才能构成刑事犯罪,而提供规避手段不能构成刑事犯罪,则《刑法》有关规避技术措施可入罪的规定几乎丧失了发挥作用的机会,也与国际立法潮流背道而驰,不可能是立法者所追求的目标。

### (三)可入罪的规避技术措施行为应包括提供规避手段

上文的分析虽然指出,2020 年《刑法》有关规避技术措施可入罪规定的立法目的不可能是只打击“直接规避”而不打击提供规避手段,然而如果 2020 年《刑法》的相关用语如同 2020 年《著作权法》对技术措施的定义那样,没有留下扩大解释的空间,则不能将 2020 年《刑法》打击的对象通过解释扩张到提供规避手段,否则将违反罪刑法定的基本原则。不过,考察 2020 年《刑法》有关规避技术措施入罪的规定在《著作权法》和《信息网络传播权保护条例》中相应的条款及它们之间的相互关系,可以得出一个结论:通过适当的法律解释方法,完全能够将提供规避手段的行为纳入可入罪的行为范围。

2020 年《著作权法》第 49 条第 2 款中有关禁止“故意制造、进口或者向公众提供主要用于避开或者破坏技术措施的装置或者部件”和“故意为他人避开或者破坏技术措施提供技术服务”的规定,照搬自《信息网络传播权保护条例》第 4 条第 2 款。如上文所述,《信息网络传播权保护条例》作为授权立法,对技术措施的保护范围不可能超越作为其上位法的 2001 年《著作权法》。2001 年《著作权法》涉及技术措施保护的唯一条款是第 47 条第(六)项,其规定了规避技术措施的法律后果——“有下列侵权行为的,……(六)未经著作权人或者与著作权有关的权利人许可,故意避开或者破坏权利人为其作品、录音录像制品等采取的保护著作权或者与著作权有关的权利的技术措施的……”。该规定中并没有出现禁止“故意制造、进口或者向公众提供主要用于避开或者破坏技术措施的装置或者部件”和“故意为他人避开或者破坏技术措施提供技术服务”的用语。然而《信息网络传播权保护条例》做出了这样的规定,说明 2001 年《著作权法》中的“故意避开或者破坏……技术措施”必然既包括“直接规避”,又包括提供规避手段。

[47] WIPO, *Guide to the Copyright and Related Rights Treaties Administered by WIPO : and Glossary of Copyright and Related Rights and Terms*, WIPO Publication No.891 (E), 2003, p. 218.

[48] “《世界知识产权组织版权条约》第 11 条规定的提供‘充分保护’的义务,看来除了要求权利人享受禁止规避行为的保护之外,还能享受禁止预备行为的保护。缔约方的国内法应当禁止为规避技术措施而制造或散发设备、产品、部件以及提供规避服务的行为。”Jörg Reinbothe and Silke von Lewinski, *The WIPO Treaties 1996: The WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty: Commentary and Legal Analysis*, Toronto: Butterworths, 2002, pp. 144—145; “那种将受禁止的行为局限于单纯规避行为,而不包括提供规避设备行为的解释,并不符合《世界知识产权组织版权条约》第 11 条的要求”, Sam Rickatson and Jane C. Ginsburg, *International Copyright and Neighbouring Rights: The Berne Convention and Beyond (2nd, Edition)*, Oxford: Oxford University Press, 2006, p. 977.

与《信息网络传播权保护条例》的规定类似,最高人民法院于2000年通过、2003年修改的《关于审理涉及计算机网络著作权纠纷案件适用法律若干问题的解释》第7条也规定了提供规避手段的法律责任。该条的内容是:“网络服务提供者明知专门用于故意避开或者破坏他人著作权技术措施的方法、设备或者材料,而上载、传播、提供的,人民法院应当根据当事人的诉讼请求和具体案情,依照著作权法第47条第(六)项的规定,追究网络服务提供者的民事侵权责任。”<sup>[49]</sup>这一条是对2001年《著作权法》有关规避技术措施法律责任的解释。作为司法解释,只能“解释”而不能改变法律的规定。如果认为2001年《著作权法》中“故意避开或者破坏……技术措施”的用语不包括提供规避手段,也将导致该司法解释在当时就失去依据,显然是不可取的。

特别需要指出的是,《世界知识产权组织版权条约》第11条和《世界知识产权组织表演和录音制品条约》第18条在规定保护技术措施的义务时,也只使用了笼统的用语“制止规避……技术措施”,并没有明确要求制止提供规避技术措施的手段。但如上文所述,对两条约的权威解释均认为制止提供规避手段是两条约要求履行的义务。两条约的缔约方在立法上的差异也只在于有的不禁止“直接规避”,但对于提供规避手段则均予以禁止。

由此可见,2001年《著作权法》有关技术措施保护的47条第(六)项(2010年《著作权法》第48条第(六)项),本身就可以被解释为同时规定了“直接规避”和提供规避手段的法律责任。2020年修改该条款时,增加列举“故意避开或者破坏技术措施的,故意制造、进口或者向他人提供主要用于避开、破坏技术措施的装置或者部件的,或者故意为他人避开或者破坏技术措施提供技术服务的”的行为,只是为了明确这一点,以省去采用法律解释方法进行推理的麻烦,并没有拓展2001年和2010年《著作权法》规定的可追究法律责任的规避技术措施的行为范围。

既然如此,对于2020年《刑法》第217条第(六)项规定的“未经著作权人或者与著作权有关的权利人许可,故意避开或者破坏权利人……的技术措施”,也完全可以进行广义解释,使之涵盖提供规避手段的行为,从而可以避免上文所述的仅将“直接规避”纳入可入罪范围所带来的各种问题,并且可以在保护技术措施方面实现“刑民衔接”。

## 四、结 语

上文虽然对《著作权法》和《刑法》有关技术措施保护范围的缺陷提出了解决方案,但过程如此大费周章,也反映出立法技术确有改进的空间。相信2020年修改《著作权法》时,立法者并不是刻意将用于计算机程序的“接触控制措施”排除出保护范围,也不是有意要对“版权保护措施”中的防复制措施和防传播措施进行区别对待。参与立法者在解释2020年《著作权法》对技术措施的定义时,所举的实例就包括被该定义排除的用于防止未经许可复制作品的“版权保

[49] 2013年1月1日,《最高人民法院关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定》生效,此处引述的《关于审理涉及计算机网络著作权纠纷案件适用法律若干问题的解释》同时废止。

护措施”——“反拷贝技术……与计算机一起配合使用、防止复制的各类‘加密狗’等”。<sup>[50]</sup> 而 2020 年修改《刑法》时，估计立法者也不希望将那些对权利人威胁最大的提供规避手段的行为排除出刑事打击的范围。然而 2020 年《著作权法》和 2020 年《刑法》相关条款的文意不仅不符合现实需要，与国际潮流背道而驰，也偏离了立法者通过修改法律提高知识产权保护水平的本意。令人遗憾的是，这种由立法技术问题造成的立法缺陷原本可以避免。

2014 年，由国家版权局负责起草，交送当时的国务院法制办公室公开征求意见的《著作权法修改草案》（简称“2014 年送审稿”）第 68 条对“技术保护措施”所下的定义是：本法所称的技术保护措施，是指权利人为防止、限制其作品、表演、录音制品或者广播电视节目被复制、浏览、欣赏、运行、改编或者通过网络传播而采取的有效技术、装置或者部件。（着重号为笔者所加）

该定义中的“为防止、限制其作品……被……运行……的有效技术、装置或者部件”就是特指用于计算机程序的“接触控制措施”，而“为防止、限制其作品……被……复制……改编……的有效技术、装置或者部件”则是“版权保护措施”中的防复制措施（改编的前提是复制）。2020 年《著作权法》如能采纳该定义，将不会出现前文所述的将计算机程序中的“接触控制措施”和“版权保护措施”中的防复制措施排除出保护范围的后果。2014 年送审稿历经 3 年的起草和反复修改，<sup>[51]</sup> 其间国家版权局两次公开征求意见，其中涉及技术措施定义的条款是在经过前期研究和多次研讨，并吸收公众意见后形成的，相对比较成熟和完善。而在 2020 年修改《著作权法》时，全国人大网分别于 4 月 30 日和 8 月 17 日公布的《著作权法修正案（草案）》第一次和第二次公开征求意见稿中，根本就没有出现对技术措施的定义。该定义是此后因“有的常委委员提出，技术措施是这次修改著作权法新增加的一种保护著作权的重要手段，明确其定义有利于法律的执行。宪法和法律委员会经研究，建议采纳上述意见”，<sup>[52]</sup> 并简单地将《信息网络传播权保护条例》中的相关条款“升格”。《著作权法》对技术措施的定义决定了技术措施受保护的范

围，对于如此重要的条款，既没有采用 2014 年送审稿中并不存在实质争议的规定，也没有给公众提出意见的机会，由此导致了上文所述的问题，不能不说是一大遗憾。

2020 年修改《刑法》时，2020 年《著作权法》已经颁布。2020 年《著作权法》有关规避技术措施的法律

责任条款明确涵盖了对技术措施提供规避手段的行为，只要《刑法》将相关表述纳入，就能保持《刑法》与《著作权法》在保护技术措施方面的无缝衔接。然而遗憾的是，2020 年《刑法》使用的是 2001 年和 2010 年《著作权法》有关规避技术措施法律责任条款中的表述，由

[50] 黄薇等，见前注[30]，第 249 页。

[51] 《著作权法》第三次修改工作于 2011 年 7 月 13 日正式启动，参见赖名芳：《〈著作权法〉第三次修订启动》，载国家版权局网站，<http://www.ncac.gov.cn/chinacopyright/contents/518/134998.html>，最后访问日期：2021 年 12 月 3 日。

[52] 2020 年 11 月 10 日十三届全国人民代表大会常务委员会第二十三次会议，全国人民代表大会宪法和法律委员会《关于〈中华人民共和国著作权法修正案（草案）〉审议结果的报告》。

此形成了可入罪的行为范围在字面上被限缩的问题,不能不说是“舍近求远”了。

著作权的保护涉及极为专业和复杂的问题,而且相关法律之间,法律与行政法规和司法解释之间应当形成相互配合的严密体系,这对立法技术提出了很高的要求。如果缺乏长期研究与反复讨论,仅在起草的最后阶段临时增加条款,或是不注意与其他法律法规之间的协调,将难以实现立法的科学化。期待《著作权法》和《刑法》尽快启动下一次修订工作,用更合理的规定、更完整的体系,对技术措施提供适当的保护。

---

**Abstract:** When the PRC Copyright Law was revised in 2020, it directly incorporated the definition of technological measures adopted by the Regulation on the Protection of the Right of Communication through Information Network, resulting in the exclusion of protection for “access control measures” to prevent unauthorized operation of computer programs and “copyright protection measures” to prevent unauthorized reproduction of works. It has caused serious consequences such as difficulty in providing effective protection for computer programs and violation of international treaties. Before revising the Copyright Law again, this problem can only be resolved through the extensive redefinition of technological measures in the Regulation on the Implementation of the Copyright Law or in the Judicial Interpretation. When the PRC Criminal Law was revised in 2020, the term incriminating circumvention of technological measures does not literally include the act of providing means to circumvent technological measures, resulting in greatly narrowing the scope of protection for technical measures and ineffectiveness of this provision. Based on the relationship between the meaning on the same terms in the Copyright Law and the Regulation on the Protection of the Right of Communication through Information, the term in the Criminal Law should be interpreted as covering the provision of means to circumvent technological measures.

**Key Words:** Technological Measures; Access Control Measures; Copyright Protection Measures; Direct Circumvention; Provision of Means to Circumvent Technological Measures

---

(责任编辑:杨 明)